กรณีศึกษา

การบุกรุกคุกคาม

เครือข่ายคอมพิวเตอร์ U.S.A.

ศ.ดร.ศรีศักดิ์ จามรมาน

บทนำ

ใน พ.ศ. 2532 มีข่าวคราวเครือข่ายคอมพิวเตอร์ทหารอเมริกันถูกไวรัสคุกคาม จนถึงขนาดต้องปิดทำการไประยะหนึ่ง ทำให้หลายคนสงสัยว่าเครือข่ายคอมพิวเตอร์ของทหารอเมริกันมีการป้องกันมั่นคงแข็งแรงเพียงใด คำตอบก็คือมั่นคงไม่ถึงร้อยละร้อย เพราะนอกจากจะโดนไวรัสโจมตีได้แล้ว ยังถูกคุกคามด้วยวิธีอื่น ๆ อีก ซึ่งในบทความนี้ได้รวบรวมตัวอย่างจากข่าวสารต่าง ๆ ใน New York Times และ Proc 10th National Computer Security Conf. เกี่ยวกับความพยายามที่จะเจาะเข้าไปในเครือข่ายโดยผู้ที่ไม่มีสิทธิ์จะใช้ ผลปรากฏว่าจากความพยายามคุกคาม 450 ครั้ง สามารถผ่านเข้าไปได้ถึง 220 ครั้งหรือประมาณร้อยละ 49 แม้จะยังเจาะไม่ลึกเท่าไร แต่ก็ถือว่าบุกรุกเข้าไปแล้ว จึงทำให้เป็นที่หวาดเสียวอยู่ทีเดียว

เครือข่ายคอมพิวเตอร์ทหารของอเมริกา

เครือข่ายคอมพิวเตอร์ทหารอเมริกันที่ใช้กันอย่างกว้างขวางนั้นชื่อว่า ดีดีเอ็น (DDN = Defense Data Network) ซึ่งอยู่ในความรับผิดชอบขององค์การวิจัยทางทหารชั้นสูง เครือข่ายนี้มีเครื่องคอมพิวเตอร์เชื่อมโยงเป็นพัน ๆ เครื่อง แบ่งออกเป็น 2 ส่วนคือ มิลเน็ต (Milnet) และ อาร์ปาเน็ต (Arpanet)

คอมพิวเตอร์ที่เชื่อมโยงกับมิลเน็ตส่วนมากเป็นคอมพิวเตอร์ของทหารอเมริกัน แต่คอมพิวเตอร์ที่เชื่อมโยงกับอาร์ปาเน็ตจะเป็นของผู้รับเหมาโครงการจ้างพัฒนาด้านทหาร ทั้งที่เป็นหน่วยงานเอกชนและสถาบันการศึกษา

ถ้าใครสามารถเจาะเข้าไปในมิลเน็ตกับอาร์ปาเน็ตได้ก็อาจจะเข้าถึงอินเตอร์เน็ต (Internet) หรือตัวแม่ข่ายใหญ่และเครือข่ายอื่น ๆ อีกมากมาย ดังนั้นจึงมีผู้ชอบการท้าทายหลายคนพยายามจะรุกล้ำเข้าไปในมิลเน็ตให้ได้

วิธีการคุกคาม

ในช่วงระยะเวลาประมาณ 10 เดือน เมื่อปี 2529-2530 ห้องปฏิบัติการลอว์เรนซ์เบิร์คเลย์ (Lawrence Berkely Laboratory) ได้ใช้เวลานาน 10 เดือน จัดทำกรณีศึกษาเกี่ยวกับการคุกคามเครือข่ายมิลเน็ต เฉพาะรายของบุคคลที่พยายามจะเชื่อมโยงคอมพิวเตอร์ของตนเข้าไปในเครือข่ายโดยผ่านคอมพิวเตอร์ลูกข่ายของมิลเน็ต

การเชื่อมโยงคอมพิวเตอร์ของใครก็ตามเข้ากับคอมพิวเตอร์ลูกข่ายในมิลเน็ต ผู้มีสิทธิ์จะต้องติดต่อเข้าไปให้ได้ แล้วพิมพ์ชื่อบัญชีและรหัสลับของตนให้ถูกต้องเสียก่อน ผู้บุกรุกทั้งหลายจึงต้องค้นหาชื่อบัญชีและรหัสลับมาทดลอง เช่น ใช้ชื่อระบบคอมพิวเตอร์ ชื่อผู้จัดการศูนย์ ชื่อผู้ใช้จากรายชื่อที่มีประกาศไว้ หรืออ่านจากจุลสารของศูนย์ ซึ่งมักจะมีชื่อผู้ใช้รวมอยู่ด้วย

ระดับการคุกคาม

ผลการรวบรวมสถิติของกรณีศึกษาในครั้งนี้ได้แบ่งระดับการคุกคามว่าประสบความสำเร็จเพียงใดไว้ 7 ระดับจากน้อยที่สุดไปหามากที่สุดดังต่อไปนี้

ระดับที่ 1 พยายามเชื่อมโยงเทอร์มินัลของตนเข้ากับคอมพิวเตอร์ลูกข่ายแต่ไม่สำเร็จเพราะสายไม่ว่าง

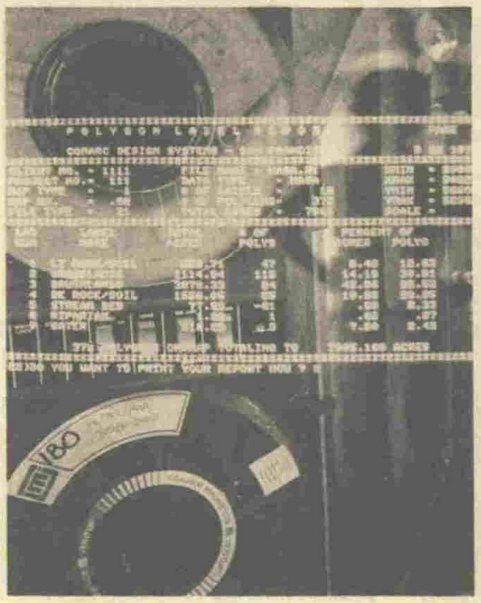
ระดับที่ 2 พยายามเชื่อมโยงเทอร์มินัลของตนเข้ากับคอมพิวเตอร์ลูกข่ายแต่ถูกปฏิเสธกลับมา

ระดับที่ 3 เชื่อมโยงได้แล้วพอระบบถามชื่อบัญชีและรหัสลับแต่เดาไม่ถูกจึงผ่านเข้าไปไม่ได้

ระดับที่ 4 เชื่อมโยงได้ เดาชื่อบัญชีและรหัสลับถูกต้อง แอบแฝงเข้าไปใช้ได้บ้าง แต่ติดขัดตรงระบบป้องกันความปลอดภัยภายในอีกชั้นหนึ่ง

ระดับที่ 5 เชื่อมโยงได้ เดาชื่อบัญชีและรหัสลับถูกต้อง สามารถใช้งานได้เป็นบางส่วนเช่น เรียกดูไปรษณีย์อิเล็กทรอนิกส์ได้ แต่สั่งใช้โปรแกรมของตนไม่ได้

ระดับที่ 6 เชื่อมโยงได้ เดาชื่อบัญชีและรหัสลับถูกต้อง สามารถเล็ดลอดเข้าไปใช้ได้เหมือนผู้ใช้ธรรมดาทั่ว ๆ ไป คือ เรียกดูข้อมูล แก้ไขข้อมูล



และสั่งงานโปรแกรมได้

ระดับที่ 7 เชื่อมโยงได้ เดาชื่อบัญชีและรหัสลับถูกต้อง สามารถทำงานได้เช่นเดียวกับนักโปรแกรมระบบ จึงทำอะไรต่ออะไรได้มากกว่าผู้ใช้ธรรมดา

สถิติจากกรณีศึกษา

หากพิจารณาดูความเพียรพยายามที่จะคุกคามระบบเครือข่ายคอมพิวเตอร์ของทหารทั้ง 450 ครั้ง จะพบว่า

1. ในจำนวน 230 ครั้งจาก 450 ครั้งหรือร้อยละ 51 ผู้บุกรุกไม่สามารถเชื่อมโยงเทอร์มินัลเข้ากับคอมพิวเตอร์ลูกข่ายได้เพราะสายไม่ว่าง กรณีนี้มิได้หมายถึงว่าการป้องกันรัดกุมดีหรืออย่างไร เพียงแต่มีผู้ใช้ติดต่อเข้ามามากจนสายไม่ว่างเท่านั้น

2. ส่วนที่เหลือ 220 ครั้งที่เชื่อมโยงเทอร์มินัลกับเครื่องคอมพิวเตอร์ลูกข่ายได้นี้ร้อยละ 5 จะถูกปฏิเสธการใช้ เพราะ DDN มีระบบป้องกันตนเองโดยเครื่องลูกข่ายสามารถทำการตรวจสอบเครื่องเทอร์มินัลที่พยายามติดต่อเข้ามานั้นว่าเป็นเครื่องที่มีสิทธิหรือไม่ นั่นคือระบบป้องกันชั้นแรกซึ่งอาศัยการระบุหมายเลขประจำเครื่องเทอร์มินัล ด้วยเหตุนี้ผู้ลักลอบที่ไม่ได้ใช้เครื่องเทอร์มินัลที่จดทะเบียนหมายเลขไว้กับคอมพิวเตอร์ลูกข่ายจะถูกปฏิเสธการเข้าสู่ระบบ

3. ร้อยละ 82 ของ 220 ครั้งที่เชื่อมโยงขั้นต้นได้ไม่สามารถผ่านระบบป้องกันชั้นที่ 2 ในการตอบชื่อบัญชีและรหัสลับ

4. เครื่องลูกข่ายของมิลเน็ตบางเครื่องยินยอมให้ใครก็ได้เชื่อมโยงเข้าไป และอนุญาตให้ถามว่ามีใครใช้เครื่องในขณะนั้นบ้าง โดยกั้นรั้วภายในไว้อีกชั้นหนึ่งบอกชื่อผู้ใช้ทุกคนที่อยู่นอกรั้ว การใช้งานอย่างอื่นจะอยู่ในรั้ว ปรากฏว่าร้อยละ 8 ของการคุกคามใน 220 ครั้งสามารถเล็ดลอดเข้ามาถึงขั้นนี้ แล้วเอารายชื่อผู้ใช้ไปประกอบการเดาชื่อบัญชีและรหัสต่อไป

5. ร้อยละ 1 จาก 220 ครั้งเชื่อมโยงเข้าไปได้ ตอบชื่อบัญชีและรหัสถูกต้องได้รับอนุญาตให้ใช้ระบบในกรณีของการเรียกดูไปรษณีย์อิเล็กทรอนิกส์ได้ จนกระทั่งมีข้อมูลที่เป็นความลับถูกเรียกไปดู เช่น ข้อมูลเกี่ยวกับยุทธวิธีทำสงครามเชื้อโรค เป็นต้น

6. ร้อยละ 2 จาก 220 ครั้ง ผู้คุกคามสามารถเดาชื่อบัญชีและรหัสลับได้ถูกต้อง ทั้งยังได้รับอนุญาตให้เข้าสู่ระบบได้เหมือนผู้ใช้ที่มีสิทธิทั่ว ๆ ไป

7. ร้อยละ 2 จาก 220 ครั้ง เป็นผู้ที่สามารถเดาชื่อบัญชีและรหัส

ลับของผู้จัดการระบบได้สามารถบุกเข้าไปใช้ได้ในฐานะผู้จัดการระบบ ทำอะไรต่อมิอะไรได้มากมาย เช่น เรียกดูรายละเอียดเกี่ยวกับผู้ใช้คนอื่น ๆ แก้ไขเปลี่ยนแปลงโปรแกรมระบบเป็นต้น

ถ้าหากจัดระดับให้เปอร์เซ็นต์ของการรุกรานตั้งแต่ข้อ 5-7 เป็นการคุกคามที่ประสบผลสำเร็จ ก็ถือได้ว่าบุคคลเหล่านั้นประสบผลสำเร็จร้อยละ 5 เหตุการณ์เช่นนี้ย่อมเป็นที่น่าหวาดกลัวไม่ใช่น้อยเลยสำหรับระบบคอมพิวเตอร์ทหารระดับชาติที่มีผู้เล็ดลอดเข้าได้ถึงร้อยละ 5

แต่ปรากฏว่าในบรรดาเครื่องคอมพิวเตอร์ลูกข่ายของมิลเน็ตจำนวน 220 เครื่องที่ถูกคุกคามนี้มีเพียง 5 รายเท่านั้นที่รู้ตัวว่าถูกแทรกแซงทั้ง ๆ ที่ความจริงแล้วลูกข่ายสามารถจะเขียนโปรแกรมเพิ่มเติมเข้าไปในระบบให้คอยสำรวจตรวจตราดูว่ามีใครพยายามจะแอบเข้ามาใช้โดยไม่มีสิทธิหรือไม่ จึงน่าแปลกใจว่าทำไมส่วนมากไม่ค่อยระมัดระวังกันบ้าง

สรุป

เหมือนลูกช่างทำรองเท้ากลับไม่มีรองเท้าจะใส่ เพราะเอาเวลาไปทำรองเท้าให้คนอื่น หรือสถาปนิกที่อยู่บ้านรก ๆ เนื่องจากไม่มีเวลาตกแต่งบ้านของตัวเองให้สวยงาม แต่สามารถตกแต่งบ้านสวยหรูให้คนอื่น นักคอมพิวเตอร์ก็เช่นกัน มัวออกแบบและจัดพัฒนาระบบให้คนอื่น เลยลืมดูแลเครื่องคอมพิวเตอร์ของตัวเอง ปล่อยให้ผู้ไม่มีสิทธิรุกล้ำเข้าไปได้

หากพิจารณาให้ละเอียดถี่ถ้วนแล้วจะพบว่า ทั้งกิจการด้านทหารและพลเรือนยังขาดทฤษฎีกับมาตรการที่ดีในการป้องกันการคุกคาม ทำนองเดียวกับไวรัสคอมพิวเตอร์ ซึ่งผู้เขียนโปรแกรมไวรัสชอบทำอะไรที่ท้าทาย ในโลกเรานี้มีผู้รักการท้าทายอีกมากมายหลายร้อยล้านคน จึงคาดได้ว่าในอนาคตจะมีผู้พยายามบุกรุกเครือข่ายคอมพิวเตอร์ต่าง ๆ อีกมากมาย

ในกรณีศึกษาที่กล่าวมานี้ผู้คุกคามใช้ความพยายามด้วยมือแล้วสามารถทำได้ชั่วโมงละ 1-3 ลูกข่าย ถ้ามีใครพยายามใช้คอมพิวเตอร์มาช่วยก็น่าจะคุกคามได้ดีขึ้น และไม่ยากจนเกินไปด้วย เช่น เขียนโปรแกรมให้ไมโครคอมพิวเตอร์โทรศัพท์ติดต่อเข้ากับคอมพิวเตอร์ลูกข่าย แล้วให้ไมโครคอมพิวเตอร์เดาชื่อบัญชีและรหัสลับ ถ้าเดาถูกก็ให้ไมโครคอมพิวเตอร์เข้าไปทำอะไรเล่นได้เลย ถ้าเดาไม่ถูกเครื่องจะหมุนโทรศัพท์หมายเลขของลูกข่ายรายต่อไป วิธีนี้อาจจะแทรกแซงได้มากกว่าชั่วโมงละ 1-3 ลูกข่ายอีกหลายเท่า

บรรณานุกรม

1. C. Stoll. What do you feed a Trojan horse? Proc. 10th National Computer Security Conf. September 1987.
2. S. Schmemann. West German computer hobbyists rummage NASA files. New York Times. 16 September 1987.